Definition of Security Practices in STP for SLMM

Tai-Hoon Kim
Dept. of Multimedia, Hannam University, Daejeon, Korea
taihoonn@hnu.ac.kr

Abstract

To manage security level of information system (IS), organizations must select security practices (SP) first, and then apply them according to security level. SP can be divided into 2 groups security management part (SMP) and security technology part (STP), and some SPs in SMP were proposed already by Drs. Tai-hoon Kim and Kouichi Sakurai [1]. In this paper, we propose some SPs in STP to construct STP for Security Level Management Model (SLMM).

1. Security Level Management and Security Practices [1]

Security level management is the activity to sustain the security level which defined as an essential one by considering operational environments of information systems. So security level management is not the check of temporary status in short time but the continuous observation to the variable environment.

To perform the security level management, all factors related to the operation of information system should be considered, and by doing so, security of whole information systems can be managed. But because of the limitation occurred by some reasons, all factors can not be managed by same level. To overcome this problem, selection of important factors should be done first.

In this paper, we propose 16 security practices, organized in 3 areas for the SMP (Security Management Part) in SLMM (Security Level Management Model). These security practices cover major areas of security countermeasures in management aspect. Additionally, more security practices organized in additional areas can be appended, and these additional practices can be drawn from the other systems engineering or security engineering areas.

The security practices were gathered from a wide range of existing materials, practices, and expertises. The practices selected represent the best existing practice of the security community, but these practices are not static and can be modified by considering characteristics and environments of information system.

Identifying security practices is complicated by the many different names for activities that are essentially the same. These activities occur anytime in the life cycle, at a different level of abstraction, or are typically performed by individuals in different roles.

An organization cannot be considered to have achieved a security practice if it is only performed during the design phase or at a single level of abstraction. SLMM does not ignore these distinctions because these can be a candidate practice organizations can select. But SLMM does not contain these practices, so security level manager should decide if they want to include these practices.

It is recommended that each security practice has some characteristics like as:

- Practice should be able to be applied across the lifecycle of the organization.
- Practice does not overlap with other practices.
- Practice represents a “best practice” of the security community.
- Practice does not simply reflect a state-of-the-art technique.
- Practice is applicable using multiple methods in multiple business contexts.
- Practice does not specify a particular method or tool.

The security practices have been organized into security areas in a way that meets a broad spectrum of security organizations. There are many ways to divide the security domain into areas.

Each security area has a set of goals that represent the expected state of an organization that is successfully implementing the security area. An organization that performs the security practices of the security area should also achieve its goals.

It is recommended that each security area has some characteristics like as:

- Security area assembles related activities in one area for ease of use
- Security area relates to valuable security services
- Security area applies across the life cycle
- Security area includes all security practices that are required to meet the goals of the security area

The 8 security areas are listed below. Note that they are listed in alphabetical order to discourage the notion that there the security areas are ordered by lifecycle phase. But in this paper, we propose the security practices related to security management part (SMP)

Part 1: Security Management Part (SMP)

- SA01 Human Resource
- SA02 Operation and Administration
- SA03 Physical Protection

Part 2: Security Technology Part (STP)

- SA04 Access Control Technology
- SA05 Cryptography Technology
- SA06 Identification and Authentication Technology
- SA07 Service Assurance Technology
- SA08 Shielding Technology

2. Security Practices in Security Technology Part

In this paper, security areas in security technology part are divided into 5 groups, such as access control, cryptography, identification and authentication, service assurance, and shielding.

Part 2: Security Technology Part (STP)

- SA04 Access Control Technology
- SA05 Cryptography Technology
- SA06 Identification and Authentication Technology
- SA07 Service Assurance Technology
- SA08 Shielding Technology

2.1. SA04 Access Control Technology

Access control can be thought of as a "super service" encompassing all security services.

The primary goal of this security area is to prevent unauthorized use, unauthorized disclosure, or modification of data by unauthorized entities. Security practices of this secure area can be used to support other security mechanism.

In SA04 Access Control Technology, there are 2 security practices

- SP.04.01 Access Control
- SP.04.02 Audit

2.1.1. SP.04.01 Access Control

Establish and manage access control technology.

Description

Access control techniques are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).

DAC is an access policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have. MAC is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified information. Role-based access control (RBAC) is an access policy determined by the system, not the owner. RBAC is used in commercial applications and also in military systems, where multi-level security requirements may also exist [2].

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- Discretionary Access Control: Comparable to UNIX permission bits

2.1.2. SP.04.02 Audit

Implement and manage audit mechanism.

Description
Audit trails (records) and logs can be checked to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations
- Re-creating security incidents

Base Requirements
- Informal reaction mechanism

2.2. SA05 Cryptography Technology

This security area contains practices relate to cryptography technology.

Cryptography is the translation of information (known as plaintext) into a coded form (known as cypertext) using a key. Cryptography is mostly used to protect the information (i.e. limit who can access the information).

In a strong cryptosystem, the original information (plaintext) can only be recovered by the use of the decryption key. So the plaintext information is protected from "prying eyes" [3]. Security practices in this area can be considered as the basic requirements.

In SA05 Cryptography Technology, there are 2 security practices

- SP.05.01 Key Length
- SP.05.02 Key Management

2.2.1. SP.05.01 Key Length

Select effective key length to protect information.

Description
After deciding cryptographic algorithm, the effective length of the key should be decided by considering security level. If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements
- public Key 512 bits
- shared (or symmetric) key 40 bits

2.2.2. SP.05.02 Key Management

Establish and manage key management infrastructure (KMI).

Description
A key management infrastructure is a set of information technology components. In this practice, the KMI performs a set of operations for internal infrastructure needs

(allocation of operations, identification and authentication of operators, etc.) and may provide complementary services for users (such as generation of authentication dual keys, or reissue of keys on behalf of users, issuing confidence dates, etc.).

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- SMI Cat X,
- 80+ exponent 512+ modulus public key length,
- 80+ hash key length

2.3. SA06 Identification and authentication technology

The security practices in this security area are related to identification and authentication technology.

Identification and authentication technology is required for effective access control. This technology usually includes a process for enabling recognition of an entity and a security measure for establishing the validity of a transmission, message, or originator or verifying an individual's eligibility to receive specific categories of information.

Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that asserts it. The I&A process assumes that there was an initial vetting of the identity, during which an authenticator was established. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier is that it must be unique within its security domain. [4][5]

In SA06 Identification and authentication technology, there are 2 security practices

- SP.06.01 Identification
- SP.06.02 Authentication

2.3.1. SP.06.01 Identification

Install and manage identification mechanism.

Description

Identification, or system identification (SID) in particular, is one way in which a system might recognize the entity (which may be a person) requesting authentication.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- unique system identifier (or ID)

2.3.2. SP.06.02 Authentication

Install and manage authentication mechanism.

Description

Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- passwords or personal identification numbers (PIN), or challenge/response exchanges

2.4. SA07 Service Assurance Technology

Service assurance has the same mean with availability. To ensure availability of data, the system must employ both preventive and recovery mechanisms.

This security area contains practices related to recovery mechanism, and other security areas contain practices related to preventive mechanism.

Availability is defined as a measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at a random point in time [6].

In SA07 Service Assurance Technology, there are 2 security practices

- SP.07.01 Redundancy
- SP.07.02 Data Recovery

2.4.1. SP.07.01 Redundancy

Consider and implement mechanism to support redundancy.

Description

Redundancy in engineering is the duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- Bypass channel available

2.4.2. SP.07.02 Data Recovery

Consider and implement mechanism to provide data recovery.

Description

Data recovery is the process of salvaging data from damaged, failed, corrupted or inaccessible primary storage media when it cannot be accessed normally.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- manual back up system

2.5. SA08 Shielding Technology

This security area contains practices related to physical and electronical shielding technology.

Tampering is the unauthorized modification that alters the proper functioning of an information security device or system in a manner that degrades the security or functionality it provides. Anti-tamper mechanisms detect such alterations [7].

TEMPEST is the investigation, study, and control of compromising emanations from telecommunications and automated information system (AIS) equipment [8].

In SA08 Shielding Technology, there are 2 security practices

- SP.08.01 Anti-tamper
- SP.08.02 TEMPEST

2.5.1. SP.08.01 Anti-tamper

Impede unapproved technology transfer, alteration of system capability, or countermeasure development.

Description

Anti-tamper encompasses the systems engineering activities intended to prevent and/or delay exploitation of critical technologies. These activities involve the entire life-cycle of systems.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- FIPS PUB 140-1 level 2
- ISO/IEC 15408 level 2

2.5.2. SP.08.02 TEMPEST

Consider and implement mechanism to prevent compromising emanations.

Description

Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose the information transmitted, received, handled, or otherwise processed by any information processing equipment.

If organization wishes to select this practice, base requirements should be satisfied.

Base Requirements

- NATO SDIP-27 Level A (formerly AMSG 720B)
- USA NSTISSAM Level I

3. Future Work

The SLMM can be divided into 2 groups, SMP and STP. By considering these 2 parts together, we can complete security level management activities.

In this paper, we propose 10 security practices, organized in 5 areas for the STP (Security Technology Part) in SLMM (Security Level Management Model). These security practices can cover major areas of security countermeasures in technology area, but not management area.

4. References

[1] Tai-hoon Kim, Kouichi Sakurai, A study on Security Level Management Model Description, International Journal of Multimedia and Ubiquitous Engineering, Vol.3 No.1, January 2008, pp.87-94

[2] http://en.wikipedia.org/wiki/Access_Control#Access_Control_Techniques

[3] http://www.boran.com/security/IT1x-7.html#Heading86

[4] http://www.iatf.net

[5] http://www.boran.com/security/IT1x-7.html#Heading111

[6] DOD3235.1H Test & Evaluation of System Reliability, Availability, and Maintainability—A Primer , March 1982. 287 Pages

[7] UK-DefStan00-43-Part1-Issue1, Reliability And Maintainability Assurance Activity Part 1: In-Service Reliability Demonstrations, January 1993

[8] http://www.at.dod.mil/index.htm